IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA
DURHAM DIVISION

KIMBERLY FARLEY, *on behalf of herself and all others similarly situated*, Plaintiff, v. EYE CARE LEADERS HOLDINGS, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Kimberly Farley ("Ms. Farley"), through her attorneys, brings this Class Action Complaint against the Defendant, Eye Care Leaders Holdings, LLC ("ECL" or "Defendant"), alleging as follows:

INTRODUCTION

1. In 2021, ECL, a record-keeping vendor for eye clinics across the country, lost control over millions of patients' highly sensitive personal information in at least four data breaches by cybercriminals (collectively, the "Data Breach"), then concealed the Breach from its customers for months. In fact, ECL has *never* notified breach victims that cybercriminals stole their information. As a result, patients across the country have no idea that cybercriminals accessed and stole their personally identifiable information ("PII") and personal health information ("PHI"), including their names, birth dates, medical record numbers, health insurance information, Social Security numbers, and care information. Indeed, ECL's customers have only just started notifying patients about the Data Breach,

meaning their information may have been exposed for up to a year without ECL warning them. Those customers are now notifying patients about the Data Breach, with each customer pointing to ECL as the cause. The number of patients affected has swelled to approximately 3 million, putting the Breach "on pace to become the largest healthcare data breach in 2022."[1]

2. On information and belief, ECL's Breach started in March 2021 when cybercriminals infiltrated ECL's systems and crippled a record-keeping system ECL provided to eye care clinics. During the breach, ECL permanently lost control over patients' PII and PHI. But despite the Breach's devastating nature, ECL obfuscated the nature of the Breach to its customers and concealed it from patients. On information and belief, ECL at first told customers the crippling attack was only a "technical issue," when it knew cybercriminals had attacked its systems with ransomware.

3. The Breach led to repeated system outages between March and April 2021, meaning that ECL could not contain the Breach's impact on its systems and patients' highly sensitive PII and PHI.

4. But before ECL could restore its systems following the March 2021 Breach, on information and belief, hackers breached its systems again just one month later in April

[1] *See Another 1.3M patients added to data breach tally of ransomware attack on Eye Care Leaders*, SC Media, https://www.scmagazine.com/analysis/ransomware/another-1-3m-patients-added-to-data-breach-tally-of-ransomware-attack-on-eye-care-leaders (last visited June 17, 2022).

2021. This second incident crippled ECL's electronic medical records systems, interrupting services and exposing still more patient PII and PHI.

5. Even so, ECL hid the Breach from its customers and patients, depriving patients an opportunity to guard themselves against the Data Breach's devastating impact.

6. On information and belief, four months after the April 2021 hack, ECL permitted yet another intrusion in August 2021. This time, a former ECL employee hacked ECL's systems because ECL did not revoke their credentials. As a result, the former employee could "wreak havoc" using those credentials.[2]

7. But ECL's data security woes did not stop there. In December 2021, ECL experienced another "security incident" that it reported to eye clinics, including Texas Tech University Health Sciences Center, EvergreenHealth, Finkelstein Eye Associates, Sylvester Eye Care, Harkins Eye Clinic, Affiliated Eye Surgeons, Chesapeake Eye, Allied Eye Physicians & Surgeons, Inc., and Shoreline Eye Group.

8. One notice from an affected clinic stated that the cybercriminals had "full access to sensitive files and databases."

9. In other words, despite experiencing data security incidents in 2021, ECL *still* failed to protect patient PII and PHI and prevent a fourth intrusion.

10. Worse yet, ECL *never* disclosed the Breach to its patients, instead keeping them in the dark while cybercriminals accessed and misused their data.

---

[2] *See Healthcare vendor accused of 'concealed' ransomware, lengthy service outages*, SC Media, https://www.scmagazine.com/analysis/incident-response/healthcare-vendor-accused-of-concealed-ransomware-lengthy-service-outages (April 20, 2022).

11. ECL's customers have only just started to notify their patients about the Breach through their own breach notices, disclosing it to millions of patients at a time. Indeed, as of June 16, 2022, the following ECL customers have disclosed breaches affecting over 2 million patients:

- TTUH Sciences Center (1.29 million patients)
- EvergreenHealth (20,533)
- Allied Eye Physicians & Surgeons (20,651)
- Summit Eye Associates (53,818)
- Affiliated Eye Surgeons (23,400)
- Northern Eye Care Associates (8,000)
- Regional Eye Associates, Inc. & Surgical Eye Center of Morgantown (194,035)
- Frank Eye Center (26,333)
- Ad Astra Eye (3,684)
- Finkelstein Eye Associates (48,587)
- Moyes Eye Center (38,000)[3]
- Sylvester Eye Care (19,377)
- Shoreline Eye Group (57,047)
- AU Health (50,631)
- Associated Ophthalmologists
- Kansas City (13,461)
- Fishman Vision (2,646)
- Burman & Zuckerbrod
- Ophthalmology Associates (1,337)
- McCoy Vision Center (33,930)
- Precision Eye Care (58,462)
- Harkins Eye Clinic (23,993)

12. Thus, the true scope and scale of the Data Breach is still unknown, as is the devastating impact it will have on patients throughout the country.

13. ECL was well-aware of the risks data breaches pose to those who store patient data, publishing an article in 2020 entitled "Why You Should Worry About Ransomware," which warns readers that "healthcare organizations are the target of a whopping 88 percent of all ransomware attacks in the U.S."[4]

---

[3] *See Another 1.3M patients added to data breach tally of ransomware attack on Eye Care Leaders*, SC Media, https://www.scmagazine.com/analysis/ransomware/another-1-3m-patients-added-to-data-breach-tally-of-ransomware-attack-on-eye-care-leaders (last visited June 17, 2022).

[4] *See Why You Should Worry About Ransomware*, https://eyecareleaders.com/eye-care-cybersecurity-ransomware (last visited June 17, 2022).

14. As a result, ECL knew it was responsible for protecting patient data well before hackers targeted its systems, also advising its website's readers on "Six Tips to Improve Patient Data Security for Healthcare Practices." Those "Tips" advised that the "best practices" to protect patient data are to: (i) Perform a security risk assessment; (ii) Train employees on data security protocols; (iii) Establish security guidelines for external devices; (iv) Assign role-based access to data; (v) Encrypt sensitive data; (vi) Build a security first culture.[5]

15. But, on information and belief, ECL adheres to none of these security practices, leading to at least four widespread data breaches in one year.

16. ECL's misconduct violates North Carolina law and harms patients across the country. Plaintiff, Kimberly Farley, is a former patient of one of ECL's customers and a Data Breach victim. Ms. Farley brings this Class Action on behalf of herself and all others harmed by ECL's misconduct.

PARTIES

17. Plaintiff, Ms. Farley, is a natural person and citizen of Tennessee, residing in White House, Tennessee, where she intends to remain. Ms. Farley is a Data Breach victim and a former patient at Summit Eye Associates ("Summit"), an ECL customer. Ms. Farley confirmed she was a Data Breach victim by calling Summit's hotline dedicated to the

[5] *See* Six Tips to Improve Patient Data Security for Healthcare Practices, https://web.archive.org/web/20201125015249/https://eyecareleaders.com/six-tips-to-improve-patient-data-security-for-healthcare-practices/ (last visited June 17, 2022).

breach, which confirms whether its patients' information was exposed in ECL's Data Breach.

18. Defendant, ECL, is a North Carolina company with its principal place of business at 2222 Sedwick Rd. Durham, North Carolina. ECL's sole "Manager" is Greg E. Lindberg. On information and belief, Lindberg was convicted of conspiracy to commit honest services wire fraud and bribery. He was sentenced to 87 months in prison.[6]

JURISDICTION & VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

20. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

21. Venue is proper under 18 U.S.C § 1391(b)(1) because ECL's principal place of business is in this District.

[6] *See Founder and Chairman of a Multinational Investment Company and a Company Consultant Convicted of Bribery and Public Corruption are Sentenced to Prison*, The United States Department of Justice, https://www.justice.gov/opa/pr/founder-and-chairman-multinational-investment-company-and-company-consultant-convicted (last visited June 17, 2022).

BACKGROUND FACTS

a. ECL

22. ECL is a practice management and record-keeping service to ophthalmology (eye care) offices throughout the United States. Its website states: "Headquartered in Durham, NC, Eye Care Leaders has brought together leading eye care companies including Integrity, iMedicWare, ManagementPlus, MDOffice, Medflow, My Vision Express, KeyMedical, IO Practiceware, and EyeDoc. We've come together with the common goal of continuing to offer and grow the best eye care solutions available anywhere in the market."[7]

23. Specifically, ECL provides record-keeping and healthcare software to eye clinics, advertising several "Solutions" for its customers:[8]

[7] *See* the "About" section on ECL's website, https://eyecareleaders.com/about-eye-care-leaders/ (June 17, 2022).
[8] See the "Services for" section on ECL's website, https://eyecareleaders.com/ophthalmologists-clinic-management-emr-ehr-software (June 17, 2022).

24. On information and belief, ECL collects and stores patient PII and PHI on its systems, assuming responsibility for safeguarding that information from breaches. Such PII and PHI includes names, birth dates, medical record numbers, health insurance information, Social Security numbers, and care information.

25. In so doing, ECL recognizes it has a duty to securely maintain patient PII and PHI, publishing several articles on how important data security is, including "Why You Should Worry About Ransomware," "4 Ways to Protect Your Practice from Ransomware Attacks," and "Six Tips to Improve Patient Data Security for Healthcare Practices."

26. These articles detail why companies that store PII and PHI have a duty to safeguard such information against theft and *how* to do so when they collect it.

27. In fact, in "4 Ways to Protect Your Practice from Ransomware Attacks," ECL advises readers that as "daunting as these attacks are, knowing what to do and what

not to do can make all the difference in whether your practice survives a ransomware attack," listing four security methods:

Get Smart About Ransomware

Education is the most effective defense. A "lack of awareness of healthcare managers regarding the sophistication of hackers" puts many practices at risk, say Campbell and co-presenter Renee Bouvelle, MD. Learn about the latest ways hackers are targeting medical practices, and familiarize your staff with the signs of ransomware:

- inability to open files
- any message about how to pay ransomware
- messages stating 'you have limited time to pay or your files will be deleted'
- a window opening to a suspicious program that you can't close.

Don't Skimp on Training

Minimize your risk for a ransomware attack by putting in the time and effort to conduct security risk assessments. Hire an outside firm or healthcare security data expert to evaluate the safety of your system each year. "You have to do something else in addition" to endpoint security, says Campbell. "This is not something that your EHR takes care of. This is not a checklist," he warns. Don't skip or shortcut HIPAA/HITECH training, developing and updating HIPAA policies and procedures, or skip developing an "emergency contingency plan." If you haven't paid attention to these things, and a breach does occur, "you can expect a lot more 'help' from the government," Campbell notes.

Keep Your Protection Current

Just like you protect your eyes from the sun with the best UV-blocking sunglasses, you need to protect your IT system with the best anti-virus and anti-malware programs available. It is common to forget or avoid software updates—they can be inconvenient and let's face it, you have more pressing things to do. But by keeping updated and upgrading when necessary, you decrease the risk of a breach that looks for known vulnerabilities in outdated versions of those programs. Your IT professional can guide you to make sure you have the right software for your system.

Build Your Team

As tempting as it may be to watch your bottom line by hiring a general "IT guy" or even a family friend to take charge of your IT department—don't. "Don't hire your cousin's brother-in-law on your mother's side or an IT company that is not trained and skilled in HIPAA, ransomware and digital forensics," warns Campbell. That's like seeing a general surgeon to remove a brain tumor, he says. The right IT professional can even conduct a "penetration test: " They act as a hacker would in order to determine exactly how vulnerable your infrastructure is to a real attack.

28. In another article, "Six Tips to Improve Patient Data Security for Healthcare Practices," ECL lists the six "Tips" as: (i) Perform a security risk assessment; (ii) Train employees on data security protocols; (iii) Establish security guidelines for external devices; (iv) Assign role-based access to data; (v) Encrypt sensitive data; (vi) Build a security first culture.[9]

29. ECL ends the article by noting that record keepers must "ensure" that they safeguard patient data:

Conclusion

Taking an all-embracing approach to patient data security may seem exhausting, but when sensitive data is at risk, following the above-mentioned best practices can ensure greater protection. For healthcare practices that are planning to take data protection seriously, HIPAA and other regulatory compliance initiatives are a good starting point for building a data security program. However, focus your efforts beyond compliance to ensure that patient data is safe and protected.

30. Even so, on information and belief, ECL adheres to none of these guidelines.

[9] *See* Six Tips to Improve Patient Data Security for Healthcare Practices, https://web.archive.org/web/20201125015249/https://eyecareleaders.com/six-tips-to-improve-patient-data-security-for-healthcare-practices/ (last visited June 17, 2022).

B. ECL fails to safeguard patient data

31. Plaintiff is a former patient with Summit.

32. As a condition to receiving eye care products and services with Summit, she was required to disclose her PII and PHI, including her name, date of birth, medical record number, health insurance information, Social Security number, and information regarding care.

33. In so doing, Plaintiff expected that her data would be securely maintained.

34. On information and belief, Summit contracts or contracted with ECL to receive ECL's record-keeping services. In so doing, ECL agreed to safeguard Plaintiff's and the Class's PII and PHI using reasonable means and according to state and federal law.

35. In 2021, ECL failed in those duties.

36. On information and belief, on March 2021, ECL experienced its first ransomware attack that affected its iMedicWare software service, interrupting ECL's services to customers. On discovering the attack, ECL knew it was a "ransomware" breach but did not disclose the breach to its customers or patients. Indeed, ECL at first referred to it as a "technical issue."

37. On information and belief, ECL "permanently" lost control over patient PII and PHI during the attack.

38. After restoring its systems to some functionality, ECL experienced another hack on April 8, 2021, with hackers once again breaching the iMedicWare software service.

39. On information and belief, the April 2021 hack also exposed patient PII and PHI to cybercriminals. Even so, ECL did not disclose the breach to patients, instead choosing to conceal it from them and obfuscate the nature of the breach to its customers.

40. On information and belief, only four months after the April 2021 hack, in July 2021, ECL experienced yet another data breach, this time targeting ECL's myCare Integrity systems. On information and belief, the hacker was a former ECL employee who still had ECL credentials because ECL did not revoke them. As a result, the former employee had access to PHI and PII even though he was not an authorized user.

41. But the intrusions did not stop there. Despite having experienced at least three breaches in 2021, ECL experienced at least one more breach in December 2021. ECL disclosed this breach to several eye care customers, including, Texas Tech University Health Sciences Center and EvergreenHealth, Finkelstein Eye Associates, Sylvester Eye Care, Harkins Eye Clinic, Affiliated Eye Surgeons, Chesapeake Eye, Allied Eye Physicians & Surgeons, Inc., and Shoreline Eye Group.

42. Thus, ECL experienced at least four data breaches in 2021, but disclosed none of them to the patients they affected. Instead, ECL left that to its customers, who only just began notifying patients about the breach this year.

43. Today, the number of reported Data Breach victims has swelled to over 3 million, including patients of those eye clinics listed above.

44. On information and belief, ECL failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over patient PII and PHI. ECL's negligence is evidenced by its failure to

prevent at least *four* data breaches in one year, in each case failing to stop cybercriminals from accessing PII and PHI. Further, ECL has refused to disclose the Data Breach to its victims, which North Carolina requires under N.C. Gen. Stat. §§ 75-61, 75-65.

45. Defendant knew or should have known its security systems were inadequate, particularly in light of the prior data breaches experienced by similar companies, and yet Defendant failed to take reasonable precautions to safeguard Plaintiff's and Class Members' PII.

46. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs.

47. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound emails using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed, and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with the least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

48. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites,

often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….

- Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it….
- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….

49. To prevent and detect cyber-attacks attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- Secure internet-facing assets
- Apply the latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;
- Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as a potential full compromise;
- Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
- Apply the principle of least-privilege
- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs

- Analyze logon events;
- Harden infrastructure
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].

50. Juxtaposed against the basic and inexpensive security measures Defendant was required to implement are the immediate, substantial, and long-lasting harms that Plaintiff and Class Members will suffer due to Defendant's conduct.

C. Plaintiff's Experience

51. Plaintiff is a former patient at an ECL customer, Summit.

52. As a condition of receiving Summit's eye care products and services, Plaintiff disclosed her PII and PHI.

53. Plaintiff provided her PII and PHI to Summit and trusted that the information would be safeguarded according to internal policies and state and federal law.

54. In March 2022, ECL informed Summit that the Data Breach affected its patients' files and information, including their names, dates of birth, medical record numbers, health insurance information, Social Security numbers, and information regarding care

55. Plaintiff confirmed she was a victim of the Data Breach by calling a hotline set up by Summit to either confirm or deny whether the Data Breach impacted patients' personal data.

56. In Summit's breach notice to patients, Summit makes clear that hackers breached only ECL's systems, and that the "incident did **not** involve unauthorized access to any Summit Eye Associates systems." (Emphasis in original).

57. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII and PHI was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

58. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII and PHI that can be directly traced to Defendant.

59. As a result of ECL's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII and PHI in their possession.

60. Stolen personal information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

61. The value of Plaintiff and the proposed Class's personal information on the black market is considerable. Stolen personal information trades on the black market for years, and criminals frequently post stolen private information openly and directly on

various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

62. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

63. One such example of criminals using personal information for profit is the development of "Fullz" packages.

64. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

65. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

66. The healthcare industry is a prime target for data breaches.

67. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[10] The next year, that number increased by nearly 45%.[11] The following year the healthcare sector was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach. [12]

68. Data breaches within the healthcare industry continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[13]

69. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[14] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to

---

[10] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"] (last accessed June 10, 2022).

[11] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Thegt Resource Center® and CyberScout®*, ITRC (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"] (last accessed June 10, 2022).

[12] *2018 End-of-Year Data Breach Report*, ITRC (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf. (last accessed June 10, 2022).

[13] *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), https://bit.ly/3LJqUr6 (last accessed June 10, 2022).

[14] *2018 End-of-Year Data Breach Report*.

restore coverage.[15] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[16]

70. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers." [17]

71. Charged with handling highly sensitive Personal Information including healthcare information, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the Personal Information that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's patients as a result of a breach. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

[15] Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), https://cnet.co/33uiV0v (last accessed June 10, 2022).

[16] *Id.*

[17] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08 (last accessed June 10, 2022).

72. Defendant disclosed the PII and PHI of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII and PHI of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII and PHI.

73. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

74. Plaintiff sues on behalf of themself and the proposed Class ("Class"), defined as follows:

> All individuals residing in the United States whose PII and PHI was compromised in the Data Breach affecting ECL, including all persons receiving notice about the Data Breach through ECL's customers.

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

75. Plaintiff reserves the right to amend the class definition.

76. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of millions of members, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII and PHI;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII and PHI;

iv. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

v. Whether the Data Breach caused Plaintiff and the Class injuries;

vi. What the proper damages measure is; and

vii. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

77. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

78. Plaintiff reallege all previous paragraphs as if fully set forth below.

79. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

80. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII and PHI —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff' and members of the Class's PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

81. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

82. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and members of the Class's personal information and PII and PHI.

83. The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII and PHI —whether by malware or otherwise.

84. PII and PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

85. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

86. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of

their bargain, lost value of their PII and PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

87. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

88. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII and PHI.

89. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' PII and PHI. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII and PHI.

90. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI Defendant had collected and stored and the

foreseeable consequences of a data breach, including, specifically, the immense damages that would result in the event of a breach, which ultimately came to pass.

91. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

92. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII and PHI.

93. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII and PHI.

94. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

95. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

96. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would

cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

97. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII and PHI; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

98. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

99. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

100. Defendant owed a duty to its patients, including Plaintiff and the Class, to keep this information confidential.

101. The unauthorized acquisition (*i.e.,* theft) by a third party of Plaintiff's and Class Members' PII and PHI is highly offensive to a reasonable person.

102. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

103. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

104. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

105. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

106. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

107. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

108. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

109. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII and PHI of Plaintiff and the Class.

110. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

111. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

112. Plaintiff and members of the Class conferred a monetary benefit upon Defendant in the form of their PII and PHI, as this was used to facilitate payment for Defendant's services.

113. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

114. As a result of Defendant's conduct, Plaintiff and members of the Class suffered actual damages in an amount to be determined at trial.

115. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Class because

Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that were mandated by federal, state, and local laws and industry standards.

116. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

DATE: June 21, 2022

Respectfully submitted,

/s/ Scott C. Harris
Scott C. Harris
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
900 W Morgan Street
Raleigh, NC 27603
Tel: (919) 600-5003
Fax: (919) 600-5035
sharris@milberg.com

/s/ Gary M. Klinger
Gary M. Klinger*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street
Suite 2100
Chicago, IL 60606
Tel.: (866) 252-0878
Email: gklinger@milberg.com

/s/ Jean S. Martin
Jean S. Martin*
Francesca Kester*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 559-4908
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Samuel J. Strauss
Samuel J. Strauss*
Raina C. Borrelli*
Alex Phillips*
TURKE & STRAUSS LLP
sam@turkestrauss.com
raina@turkestrauss.com
alexp@turkestrauss.com
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

ATTORNEYS FOR PLAINTIFF

* *pro hac vice forthcoming*